

our networks as basic good cyber hygiene was actually a security breach.

This technique and the breadth of this hack are both unprecedented, and it shows that the Federal Government is still far from where we need to be to handle the cyber security challenges of the 21st century.

As the Permanent Subcommittee on Investigations said in its investigation and report, these alarms that we have been raising over time are ones that we should have paid attention to. In 2019, last summer, Senator CARPER and I issued a shocking report that detailed the unacceptable cyber security vulnerabilities in the Federal Government—vulnerabilities that may very well have played a role in the extent of this breach.

Our report looked back at how well Federal agencies complied with basic cyber security standards over the past decade. Every agency we reviewed failed. And we know that four of those agencies—the Department of Homeland Security, the State Department, the Department of Agriculture, the Department of Health and Human Services—are among those that have been breached in this current cyber attack.

That report from the Permanent Subcommittee on Investigations made clear that Federal agencies were a target for cyber criminals and other nation-state adversaries. In 2017 alone, Federal agencies reported 35,277 cyber incidents. It is the most recent data we have—in 1 year. The number of cyber incidents in 2019 was a little bit less, 28,581. But 2020 will bring what is likely the biggest, most comprehensive breach across the Federal Government in our history.

We also found we are not equipped to handle this threat. Many of the agencies we reviewed didn't even know what applications and platforms were operating on its systems. That begs the question: How can you protect something if you don't even know what you need to protect?

If Federal agencies fail at meeting basic cyber standards, there is no way they are equipped to thwart the kind of sophisticated attack that apparently happened over the past several months. Here, the attackers were meticulous and had a detailed understanding of how to evade intrusion detection practices and technologies. And because the Federal agencies involved were unprepared, the attackers had ample time to cover their tracks, which means evaluating the extent of the damage and kicking them off our networks is going to be incredibly difficult and time-consuming.

Given how widespread this attack is and how much wider it is expected to become, it certainly seems like the Federal Government's current cyber resources are going to be spread incredibly thin.

Congress and the executive branch have failed to prioritize cyber security, and now we find ourselves vulnerable and exposed. We have to do better than

this. This breach has to be a wake-up call for all of us.

Over the years, I have worked across the aisle with Senator PETERS, Senator CORNYN, Senator HASSAN, and others on legislation to beef up our Federal Government cyber capacities, including the Risk-Informed Spending for Cybersecurity Act, the Federal System Incident Response Act, and the DHS Cyber Hunt and Incident Response Team Act, and others. We are proud of this legislation.

Let's be honest. It wasn't enough. We need to do more. We need to not only defend our networks but go on the offense to defer a nation-state, like Russia, and nonstate actors from even considering a future attack like this. That means there needs to be consequences for cyber attacks significant enough to prevent them from happening again and a willingness to act preemptively when warranted.

Congress has to take a hard look at the cyber security capabilities of our Federal agencies. In the next Congress, I will be the top Republican on the Senate Homeland Security and Governmental Affairs Committee, which means I will either serve as its chairman or ranking member, depending on the outcome of a couple of races in Georgia. Senator PETERS will be the chair if the Democrats take the majority. I will tell you here tonight, whether I am chairman in January or him, we intend to hold in-depth hearings on cyber security. With what has happened, we will also, of course, focus on the origin, scope, and severity of this breach.

Actually, 3 weeks ago, even before this attack was revealed, we met and decided to hold these cyber security hearings, and we are already working on comprehensive legislation to improve our cyber defenses in the Federal Government going forward.

We must now move with a renewed sense of purpose and urgency to learn from this massive attack. We have to remove these hackers from these systems and put in place protections to prevent it from happening again.

As this cyber attack has made clear, we have to redouble our efforts to shore up our defenses. We are two decades into the 21st century, but most of the Federal Government legacy computer systems are from the 20th century. Federal agencies are simply behind the times when it comes to defending themselves against these threats posed in cyber space. The government is trying to respond to sophisticated, 21st century attacks with 20th century defenses. This attack has shown us the consequences of that and should be the catalyst for real bipartisan action here in the next Congress to better defend networks that contain sensitive, personal information, and other information critical to our economy, our healthcare, and the safety and security of all Americans.

I yield the floor.

The PRESIDING OFFICER (Mr. TILLIS). The Senator from Ohio.

Mr. PORTMAN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. BENNET. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

CORONAVIRUS

Mr. BENNET. Mr. President, before I give my remarks, I would like to say that I hope the rumors are true that we are getting close to a deal here. The country needs us to reach a bipartisan deal, as we did in March, unanimously, when we passed the CARES Act here.

It is time for us to do that again. In Colorado and all across the country cases are spiking and the economy is slowing down. People need relief. They need help. I hope we will come together in a bipartisan way and do that.

I hope that the deal is not going to come crashing down because of a disagreement about what the Federal Reserve's authority ought to be under the 13(3) program. That is an important program for the Federal Reserve to help when things are really distressed in our economy—to help our small businesses, our State and local governments, and working families all over this country.

It is an authority that Donald Trump used—or that the Fed used while Donald Trump was President. People on both sides of the aisle said it was an effective authority, and if it is an effective authority for President Trump, it should not be taken away from the Federal Reserve just because Joe Biden is becoming President of the United States.

So I hope that we will come to an agreement. I expect that we will. I hope it is soon. People need the help.

CYBER SECURITY

Mr. President, in the last few days we have learned that the United States was subject to one of the most brazen cyber hacks in history. Based on press reports alone, the hackers appear to have breached the Department of State, the Department of Commerce, the Department of Energy, the Department of the Treasury, the National Nuclear Security Agency, and the Department of Homeland Security—including the agency responsible for our cyber security.

On top of that, the hackers also managed to breach major American companies like Microsoft and compromised several State governments and other foreign governments all at the same time in this process.

While we are learning more about these breaches, the level of resources and sophistication bears all the hallmarks of Russia. Reports suggest that the hackers have been in the system since the spring and perhaps much longer. According to public reports, they may still be in our system tonight.

We have heard literally not a word from the White House about this, not a single word from the President about this. I suppose this should come as no surprise. After all, this is the same President who, to this day, refuses to acknowledge that the Russians interfered in our 2016 election even though our intelligence agencies unanimously agree that Russia meddled.

This is the same President who went to Helsinki and, on foreign soil, sided with Russian President Vladimir Putin, a former KGB officer, over the CIA, the FBI, the NSA, and all of our other intelligence organizations.

The same President who spends the lion's share of almost every day criticizing everyone from the National Football League to Greta Thunberg, who is 17 years old, to the Secretary of State in Georgia for upholding the rule of law can't bring himself to utter one word of criticism for Vladimir Putin—the same President who, instead of challenging Putin, proposed creating a joint cyber unit between the United States and Russia. That would be like asking a burglar to design the locks on the front door of your house.

The Trump administration is not known for its consistency, but here is the one place they have been resolute and consistently weak, coddling dictators and abandoning our democratic allies.

As a member of the Intelligence Committee, I can't say for sure today whether this weakness emboldened or enabled our adversaries. We are going to have to study the facts. But the administration's abject fecklessness certainly hasn't helped.

To understand how weak the Trump administration has left us, it is important to appreciate the wreckage of their total war on the Federal Government. They came into office with a promise to dismantle “the administrative state,” but what they ended up doing was dismantling our national defenses.

Over the past 4 years, the administration drove thousands of qualified public servants to the exit, including cyber security experts in agency after agency critical to our national security.

Back in March, I asked the Department of Homeland Security to detail its plans to shore up our cyber security. They responded by telling me that they still had hundreds of vacancies for cyber security.

President Trump eliminated the top coordinator for cyber security at the National Security Council. There is no one, therefore, coordinating our cyber defenses across the Federal Government or engaging the private sector to make sure we are working together to shore up those vulnerabilities.

If you put it all together, we have been left with a gutted bureaucracy without the necessary leadership to respond to cyber threats and espionage in a coherent way. And a few weeks ago, the President fired Chris Krebs, just to

make matters worse, our top Department of Homeland Security official for domestic cyber security—the very person who would be leading our response to the hacks right now.

But he is gone. He is gone not because he did a bad job but because he refused to repeat the President's baseless claims about fraud in the election, claims the President is still making as we meet here tonight more than 6 weeks after the election and 4 days after the electoral college confirmed Joe Biden's election.

In the last few days alone, the President has tweeted at least 25 times about fraud in the 2020 election, something he has completely invented in his mind, but he hasn't said one word about the most far-reaching breach of cyber security in our history by a foreign adversary.

As we meet here again tonight in the land of flickering lights, uncertain whether we will pass a budget to keep the lights on in our exercise of self-government for the weekend, all across the globe there are public servants, the men and women of our intelligence services, who are working to repair the damage that has been done and to keep us safe. They deserve and the American people deserve a President who makes clear that we won't tolerate intrusions like this, a President who rallies our allies to our common cause.

If we have learned anything this year, it is that our government has proven itself woefully unprepared to deal with emerging threats, not only a cyber attack but also a global pandemic. This year has also taught us that the cost of ignoring these threats is much, much greater than the cost of addressing them head-on.

But to do that we need a President who doesn't bury his head in the sand or his face in Twitter, a democracy that can think beyond the next commercial break on cable news, that can put aside festering partisanship and forge an enduring national security policy for the 21st century.

And Russia is not our only concern. I can assure you that China is not chasing the latest controversy on Twitter or cable news. They are building roads and bridges and airports across the globe. They are laying fiber-optic cables beneath the ocean. They are competing with us in space. They are forging new alliances and pioneering new technologies every month. They are making considered choices to shape the 21st century while we are struggling here to keep the lights on.

This lack of concern from the White House about this breach is a dark moment, but soon we will have the chance to take another approach. I hope everyone in this Chamber will seize the opportunity to work with one another to secure the promise of our great country for the next generation and America's role in the world.

I yield the floor.

The PRESIDING OFFICER. The Senator from Kansas.

EXECUTIVE CALENDAR

Mr. ROBERTS. Mr. President, I ask unanimous consent that the cloture motion with respect to Calendar No. 836 be withdrawn and the Senate proceed to the consideration of the nomination.

PRESIDING OFFICER. Without objection, it is so ordered.

The cloture motion was withdrawn.

The PRESIDING OFFICER. The clerk will report the nomination.

The senior assistant legislative clerk read the nomination of Charles A. Stones, of Kansas, to be a Member of the Board of Directors of the Federal Agricultural Mortgage Corporation.

Mr. ROBERTS. I ask unanimous consent that the Senate vote on the nomination with no intervening action or debate; that if confirmed, the motion to reconsider be made and laid upon the table; and that the President be immediately notified of the Senate's action.

The PRESIDING OFFICER. Without objection, it is so ordered.

The question, Will the Senate advise and consent to the Stones nomination?

The nomination was confirmed.

The PRESIDING OFFICER. The majority leader.

CORONAVIRUS

Mr. MCCONNELL. I think that all of our colleagues understand our present situation.

Both sides of the aisle are firmly committed to finalizing another major pandemic rescue package for the American people. Constant discussions have been underway for several days now.

As of right now, we have not yet reached a final agreement, regretfully. I believe all sides feel we are making good progress on a major relief bill that would travel with a full-year appropriations measure.

But, alas, we are not there yet.

Given that, our urgent task is to pass a stopgap government funding measure. There is no reason the Federal Government funding should lapse while we hammer out our remaining differences. We are going to take up the continuing resolution, which just passed the House a few minutes ago on an overwhelming bipartisan basis.

I hope this body will pass it easily and get this measure on the President's desk so Congress can complete our negotiations with no pointless lapse in normal government operations.

LEGISLATIVE SESSION

MORNING BUSINESS

Mr. MCCONNELL. Mr. President, I ask unanimous consent that the Senate proceed to legislative session and be in a period of morning business, with Senators permitted to speak therein for up to 10 minutes each.

The PRESIDING OFFICER. Without objection, it is so ordered.